Conclusions and recommendations

de Hert, Paul; Koops, Bert-Jaap; Leenes, Ronald

Published in:
Constitutional rights and new technologies

Publication date:
2007

Document Version
Other version

9. Conclusions and Recommendations

Paul de Hert,[1] Bert-Jaap Koops[2] and Ronald Leenes[3]

9.1. General

This book contains seven country reports, covering Belgium, Canada, France, Germany, the Netherlands, Sweden, and the US. Every chapter studies the changes in constitutional rights and human-rights policy related to developments in ICT and other new technologies. The main focus is on the constitutional rights to privacy and data protection, inviolability of the body, inviolability of the home, secrecy of communication, and freedom of expression. As mentioned in the introduction, this study is a sequel to an earlier study carried out in 1999-2000 under supervision of Alis Koekkoek of Tilburg University.[4] The present study contains the same countries as the Koekkoek report, extended with a chapter on the Netherlands. The central question in the present study is to identify which developments have taken place in the countries at issue with respect to constitutional rights and new technologies, in particular since 2000. Knowledge of these developments may help countries in adapting or updating their Constitution, as it provides inspiration for diverging strategies to achieve functionally equivalent results, i.e., the continued protection of the widely shared constitutional values of privacy and freedom of expression.

9.2. General constitutional characteristics and developments

9.2.1. Little constitutional dynamics as a general trend

A first sub-question dealt with in all the country reports is general and concerns the nature and main characteristics of the six constitutional systems and the changes therein, in particular since 2000, for instance with respect to constitutional review, horizontal effect, or the influence of international law. The chapters show that there are several constitutional systems with hardly any change, and a few with some dynamics.[5] The US is an example of a very stable system. Their 'rigid' constitution is very steadfast, and no significant amendments have been added or proposed. The Supreme Court has produced several relevant judgments that keep the interpretation of the Constitution up-to-date in light of technological developments. The Netherlands is an example of a country where considerable debate has taken place on amending the Constitution in light of the 'digital age', but even there, despite several Bills having been drafted, the

---

1 Paul de Hert is Associate Professor in Law & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands, and Professor at Law, Science, Technology & Society (LSTS), Free University of Brussels, Belgium.

2 Bert-Jaap Koops is Professor in Regulation & Technology at TILT.

3 Ronald Leenes is Associate Professor in Law & Technology at TILT.

4 A. Koekkoek, et al. 2000.

5 A similar conclusion was drawn by Franken and Koekkoek 2006 on the basis of a survey of Canada, Denmark, Japan,

to appear in: Ronald Leenes, Bert-Jaap koops (eds), CONSTITUTIONAL RIGHTS AND NEW TECHNOLOGIES: A Comparative Study Covering the United States, Canada, France, Germany, Belgium, the Netherlands, Sweden, The Hague: T.M.C. Asser, 2007

Constitution has yet to be amended. Belgium is an example of a country that used to be very static from a constitutional point of view, but has started to incorporate many changes. Its original 1831 Constitution has received several important revisions between 1970-1993 in order to transform the Unitarian state into a federal state with a plurality of legislative bodies with distinct competences, and governments. In addition, the Constitution was enriched with certain fundamental rights relevant to this study in 1993-1994 and in 2000. Moreover, the Court of Arbitration, operational since 1984 as an arbiter between the different legislative bodies, became a full Constitutional Court in 2004. Even in Belgium, however, technological developments have not been a primary trigger for constitutional amendments, and the fact that this country has been the most dynamic in constitutional change since 2000 among the countries surveyed in this book, indicates that new technologies have overall had little impact on constitutional changes over the past years.

The lack of profound constitutional changes in the countries surveyed has without doubt an institutional logic. Constitutions generally have a 'rigid' status and are not meant to be amended or altered swiftly. This seems to be even more the case in federal systems with a delicate power balance between different governments. The US, for example, where the Constitution is still in function more or less in its original form, is a case in point. The Canadian fundamental rights, as formulated in the Canadian Charter of Rights and Freedoms (Part I of the Constitution Act, 1982), are extremely difficult to amend, since the consent of the Parliament is needed together with the agreement of seven to ten provincial legislative assemblies representing more than 50 percent of the population.[6]

Another reason that none of the countries have undergone profound constitutional changes due to the emergence of new technologies, is that most constitutional rights, unlike Article 7 and 13 of the Dutch Constitution, are drafted in general terms broad enough to encompass new technologies. Freedom of expression and the right to secrecy of communications, for example, are usually worded in a technology-neutral way or, for instance in Sweden, with open endings like 'and other technical recordings' and 'or other confidential communications'. Many country reporters stress the importance of technology neutrality in constitutional protection, given the usually complex process of amending the Constitution. At the same time, as Magnusson Sjöberg warns, technology neutrality poses the risk of constitutional rights becoming very vague and thereby diluting constitutional protection. In that respect, open-ended formulations are to be preferred over overall abstract formulations.[7]

Still, the technology neutrality of most constitutional rights does not account wholly for the lack of dynamics. The chapters seem to suggest that developments in ICT and new technologies are often not looked at a from a constitutional or human-rights perspective, perhaps with the exception of general privacy issues. This seems to be especially the case for countries with older constitutions (Sweden, the US, Belgium, and the Netherlands). These texts often tend to be smaller, more concise and less value-driven.

---

6 See also Franken and Koekkoek 2006, p. 1162.

7 On the pros and cons of technology neutrality and strategies to deal with the trade-off between sustainability of law and legal certainty, see Koops 2006.

The more pragmatic approach of Belgium contrasts heavily with the more principled approach of Germany and France, for instance in the area of biomedical technologies. It is not possible at this stage to assess these differences. One could also hold that the seemingly pragmatic approach in Belgium is inspired by the liberal value of freedom (e.g., to sell one's organs or to alter one's body) that dominated most nineteenth-century Constitutions.

The impression nevertheless remains: technology seemingly produces little constitutional dynamics. This is not to say that constitutions are entirely dormant. In France and Germany, for example, constitutional rights play a fairly active role in debates. In Germany, this is due to the presence of many (post-Wold War II) value-driven constitutional rights, whereas in France, this results from more procedural basic rules, such as the rule that the legislator is obliged to define the guarantees to the exercise of fundamental rights and liberties. Hesitations by the legislator to fulfil this role account for most of the constitutional case-law produced by the French Constitutional Council in the area of new technologies.

9.2.2. The impact of international legal instruments

International human-rights treaties such as the European Convention of Human Rights and Fundamental Freedoms (1950) and the UN International Covenant on Civil and Political Rights (1966) play an important role in the constitutional tradition of the European countries in this survey. In Belgium, France, Germany, and the Netherlands, directly binding rights from international treaties, which are sometimes absent in the national constitutions, play a major role. The ECHR is more specific with regard to the possibilities for limitation, whereas the national constitutions tend to emphasise the existence of rights as such and usually do not go beyond the requirement that limitations have to have a legal basis.

Although not all of these European countries belong to the monist tradition (like the Netherlands), they are all eager to have cases decided in accordance with the case-law of the European Court of Human Rights. This situation stands in a striking contrast with the ethics of the US Supreme Court which, as a rule, does not refer to international treaties or case-law of foreign or international courts. Limitations to US constitutional rights do not resemble the European approach. The First Amendment with regard to freedom of expression omits every mention of the possibility to restrict this right, and the Fourth Amendment has its own particular requirements regarding limitations.

The open attitude in the European reporting countries also concerns acts and initiatives generated not by the Council of Europe, but by the European Union. Very often, ordinary legislation with regard to technological developments is enacted as a result of obligations created by regulations and directives (first pillar) or by decisions and framework decisions (third pillar). The position of the French Constitutional Council *not* to supervise national laws that implement European initiatives might be problematic from a constitutional point of view with regard to third-pillar 'laws' enacted without co-decision power of the European Parliament and without effective judicial control by the European Court of Justice.[8] However that may be, the omnipresence of the European law-maker in

[8] See on this, De Hert 2004.

areas affected by technological change likely also contributes to the lack of national constitutional activity discussed above.

9.2.3. Constitutional review

We have already observed that most reporting countries have constitutional rights with an open texture that apply in one way or another to the use of new technologies. In addition, all reporting countries have a system of constitutional review, ranging from unlimited variants, such as the US (all courts without limitation in time), to more limited variants, such as France (only the Constitutional Council before or six months after adoption of the text of the law). The chapters do not allow concluding on the eligibility of a particular form of constitutional review. From a theoretical perspective, one could argue that the continuous development of technology does not allow a court to decide on the constitutional nature of a given law in too short a period of time, but this argument is not supported in practice by the French chapter, which shows an active constitutional court unhampered by the requirement to demand constitutional review within six months of enactment of a law.

What the chapters do show, however, is the importance of having one form of constitutional review or other in the first place, and this is a major point of attention for the Netherlands. Particularly now that Belgium has recently opted for a fairly broad form of constitutional review, the Netherlands have become rather isolated on the Western constitutional scene by their prohibition of constitutional review (Art. 120 Gw). Despite recommendations by the Koekkoek report, the CFRDA, and the 'National Convention', constitutional review is still not possible in the Netherlands.[9] As constitutions are amended to update the constitutional rights in light of new technologies – particularly if they are made considerably technology-neutral, like intended in the Dutch proposals, and hence give less concrete guidance with respect to specific technological developments –, constitutional review is an important safeguard for effectuating constitutional protection in actual practice.

Having said this, it should be noted that constitutional review does not solve all problems. It allows the courts to keep the Constitution alive and to keep a check on the legislative activities of the legislature, but it can also function as a restraint on constitutional vitality. The US chapter clearly spells out a backward evolution with regard to judicial activism: most of the expanding interpretations of existing rights are set back by the present Court with its more conservative composition. Effective human-rights protection therefore cannot rely solely on the eagerness of judges to apply constitutional principles to the society of today. Judges also need to work on the basis of constitutional texts and principles that guide them through their work, and hence, constitutions should have truly guiding principles and should not become too abstract or too general.

9.2.4. Horizontal effect

Technology is not an instrument specifically for governments; citizens depend on the use of technology at least as much. None of the constitutions of the reporting countries, however, contain any clause relating to the horizontal effect of fundamental rights.[10] Constitutional law seems to be devised as an instrument to regulate vertical relations

---

[9] See *supra* 6.3, with references.

[10] See also Franken and Koekkoek 2006, p. 1155.

and to protect citizen against governmental power abuses. It is clear that similar power abuses can occur by private actors, including businesses, but this has not had a clear effect on constitutional protection at large. Most reporting countries address the issue of horizontal effect by assuming in one way or another that it is up to the legislator to convert fundamental-rights protection into specific legal norms that apply between citizens, for example in data-protection acts.

9.3. Privacy

9.3.1. General

The right to privacy is not explicitly mentioned in the Canadian, US, France, German, and Swedish constitutions, but it is recognised as being a part of the constitutional heritage in all the reporting countries. Belgium has, like the Netherlands, a general privacy right, albeit of a more recent date. The 1994 insertion of this right in Article 22 of the Belgian Constitution is remarkable, but in line with our observation above that constitutions in Europe tend to be sparing in possibilities to limit rights: it copies the general wordings of the right as formulated in Article 8 paragraph 1 ECHR, but omits the limitation grounds of paragraph 2 of this article. When Belgium adopted the amendment, it was asserted that the right and its limits should be understood along the lines of the ECHR and its case-law. It is unclear whether such a use of supranational constitutional law at the expense of national constitutional law is ultimately beneficial to privacy protection. Given the fact that many chapters indicate that proportionality is at the heart of constitution-related privacy debates, it can be recommended to codify at least this criterion, if not other elements of Article 8 ECHR, in national constitutions, as an unequivocal order to the legislator to explain the proportionality of proposed privacy-infringing laws.

Privacy in general is expressed in different terms and is constructed differently in the reporting countries. In Germany, where neither privacy nor data protection are mentioned in the Constitution, its source is Article 2 paragraph 1 (liberty) and Article 1 (human dignity). In France, the source of privacy is not human dignity but liberty. Besides an implicit recognition by the Council in 1997, privacy was more explicitly recognised in French constitutional law in 1995-1999 as a part of the more generic right to individual liberty (Art. 66 Constitution) and rooted in Article 2 of the 1789 Declaration of Man and the Citizen: the right to liberty as an unalienable human right.

It is hard to assess the implications of these different expressions of the right to privacy and to put into question the formulation of the right to privacy as an independent right in the ECHR and in the Dutch and Belgian constitutions. It is neverthelss clear that the choice of Article 1 of the German Constitution (hereinafter: GG) as a source for the right to privacy is important for its strong position in German constitutional law. The US chapter clearly demonstrates the weakness of privacy when it is not provided for explicitly in the constitution: privacy protection is built up and broken down by judges and can therefore fluctuate significantly.

The main constitutional provision in both Canada and the US where privacy is read into, is the provision protecting against unreasonable search and seizure. The chapters

suggest that this right is formulated in terms that are perhaps too physical, but the cases quoted show that the wordings are (still?) open enough for the courts to apply them in a rapidly changing world. A crucial element in both rights is that they protect people, not places. This approach has significant advantages in a technology-driven world where traditional notions of place become blurred. In a world of Ambient Intelligence, 'place' becomes something centering on people rather than on physical objects or geographical locations, since the surroundings change along with the people acting in them.[11]

Courts in Canada and the US also use the criterion of 'reasonable expectations of privacy' to determine whether certain measures are unreasonable. Its application, especially in the US, seems rather tricky for privacy protection in a rapidly changing world where technology permeates everyday life. As technology develops, the 'reasonable expectation of privacy' develops along with it, generally to the detriment of privacy as technology of itself tends to decrease privacy expectations.[12] An example is the *Kyllo* case in the US, where the Supreme Court used the criterion of a device being 'in general use' to determine whether or not it infringed privacy;[13] as most technology applications tend to develop from limited, sectoral use to general, public use, the related privacy expectations at one point in time will become unreasonable. Hence, using 'reasonable expectations of privacy' to face developments in technology poses the risk of a slow but certain erosion of privacy. Although the criterion is not wholly absent in the case-law of the European Court of Human Rights,[14] courts and legislatures should be cautious in applying it in the field of technology law.

9.3.2. Data protection

Recently, the role of data protection proper has received constitutional recognition in the EU Charter of fundamental rights of the European Union.[15] In the Charter, a separate right to data protection has been recognised apart from a right to a private life for the individual. The right to have personal data protected is, however, not explicitly mentioned in most constitutions of the reporting states, with the exception of Sweden (Ch. 2, Art. 3, para. 2 Instrument of Government) and the Netherlands (Art. 10 paras. 2-3 Gw). Nevertheless, it is recognised as part of the constitutional heritage in all the reporting countries, and the incorporation in the EU Charter may be a sign of growing recognition for data protection as a constitutional right. Whether it will further develop as an autonomous right independent from privacy[16] remains to be seen: the chapters show that in most countries, data protection is (still) largely discussed in the context of privacy.

In Germany, the right to informational self-determination is a stand-alone right next to privacy. In France and Canada, the data-protection laws have a quasi-constitutional

---

11 See also *infra* 9.3.3.

12 See Koops and Leenes 2005.

13 See *supra* 8.4.2.

14 ECHR, *Halford* v. *United Kingdom,* judgment of 25 June 1997, § 42. See also, generally, Nouwt, et al. 2005.

15 See http://europa.eu.int/comm/justice_home/unit/charte/en/charter02.html.

16 As recommended by some scholars, e.g., Blok 2002.

status. The French Data Protection Act is of a general nature. In Canada, the 1983 Privacy Act was designed to protect personal data in the federal public sector, whereas the 2000 Personal Information Protection and Electronic Documents Act was enacted to protect personal information in the private sector; only the first has quasi-constitutional value (it will trump other laws unless the other act addresses the privacy issues), the latter has the status of ordinary legislation. The 1995 EC Data Protection Directive primarily provides data protection in the European reporting countries.[17] Whereas Canada has responded to this initiative by enacting similar legislation, the US has refrained from adopting general ordinary data-protection legislation. In US law, however, some basic principles of data protection familiar to the Canadian and European regulations are absent. As soon as one gives data away or shares them, legal protection stops. The purpose-limitation principle, i.e., the principle that data should be collected and processed according to a predefined goal or purpose, has not found firm ground in the US tradition.

All chapters show the overall importance of data-protection principles as yardsticks to measure new developments. Constitutionalisation of these principles, in the line of the EU Charter, is therefore to be recommended. In that respect, it is worth mentioning that the protection of the EU Charter is more specific and more inclusive than the protection in the Dutch Constitution (Art. 10 para. 3 Gw), which does not, for instance, mention the role of the Data Protection Authority. Generally, one senses a reluctance of courts in many countries to apply data-protection principles to their fullest extent. This is partly compensated by the activities of the national Data Protection Authorities.[18] In the line of the EU Charter, it can therefore be recommend to give these institutes constitutional recognition. Also, the pivotal role of the purpose-limitation principle in many debates, e.g., the debate about privacy versus security, also suggests that this principle should be part of the constitutional codification of data protection.

Culture seems to be a factor of importance with regard to data protection. Although Sweden was the first state (after the German Land of Hessen) to enact a national data-protection act (1973) and although Chapter 2, Article 3 of the Instrument of Government recognises that 'every citizen shall be protected against any violation of integrity by automatic processing', Swedish constitutionalism is dominated by the notion of transparency and access to government information. Sweden therefore struggles with the main principles of the European Data Protection Directive and is now proposing a more US-like data-protection regulation that does not focus on prevention, but on data abuse. The Swedish development warrants closer scrutiny: it can be questioned whether the European data-protection system, with its focus on *a priori* regulation of data collection and processing, can be upheld much longer in a world where data processing occurs in so many ways, to such an extent, and for so many purposes as it does today. Shifting the focus of legal protection to *a posteriori* regulation of data abuse might turn out to be a better strategy to protect individuals in the long run.

In all reporting countries, specific issues have determined the constitutional privacy and data-protection agenda. These overlap only partially, except with regard to the issue of balancing privacy and security, which has triggered significant debates and legislative

---

17 See also Franken and Koekkoek, p. 1160.

18 In France, for example, the Data Protection Act is acknowledged as law which guarantees a constitutional right, but the control of it by the Constitutional Council is weak. The Council only formally controls whether other laws respect the data-protection guarantees and principles established by the Data protection Act. In reality, control is therefore realised by the CNIL.

activity in all countries. As a consequence of the September 11 attacks, many countries have adopted anti-terrorist laws, often but not always technology-related, that infringe privacy or data-protection principles. The chapters show some resistance by the constitutional courts against overintrusive government powers, for instance in Germany, where the Constitutional Court has tied video surveillance in public places to the requirement that there are objective indications of dangerousness of the place to be monitored. Also, some cases have taken into account the proportionality criterion in dealing with proposed measures. In general, however, constitutional rights have not functioned to substantially limit or block legislative proposals to extend government powers to enhance security. At the same time, it should be noted that in several countries, the move towards more security measures to the detriment of privacy started already before 9/11, even if the terrorist attacks seems to have speeded up certain measures.

Besides 'security versus privacy', the following themes have been mentioned in the chapters: video surveillance (France, Germany, Belgium), the use of cameras on highways (France), electronic surveillance or the e-bracelet (France), biometrics (France), the processing of location data (France), profiling (the Netherlands), the impact of antiterrorism laws on other states (Canada), privacy competences of provinces in federal states (Canada, Belgium), access to government information versus data protection (Sweden), workplace privacy (Sweden), and genetic testing (Belgium, US).

9.3.3. Inviolability of the home

The inviolability of the home is covered explicitly as such in most European constitutions except the French, and via the protection against unreasonable searches in the Canadian and US systems. Although these provisions have not triggered much debate in the reporting countries with regard to technological developments, two observations can be made.

The first regards the source of these provisions. Whereas French constitutional law considers the right to have the home protected as a component of individual liberty (Art. 66), most other systems identify privacy as a basic value underlying the protection of the home. This view certainly corroborates the observation that if there is an inner and outer sphere of privacy, then the home belongs to the most inner sphere (in the German term: Kernbereich) of privacy. It is not unproblematic, however. Indeed, the right to have the home protected is much older in legal history than the right to privacy, which was only recognised as such in twentieth-century constitutions. In the nineteenth century, it was therefore held that the right to property was at the core of the values underlying the protection of the house. It is unclear from a digital-rights perspective whether the right to inviolability of the home should be conceived as an independent right based on a plurality of values (liberty, property, privacy, etc.) or as a privacy-specific right protecting not bricks but people. This issue certainly merits further debate.

Second, linked to the foregoing, it appears that the current conception and wordings of the right to inviolability of the home is not technology-proof. The chapters identify problems with regular video surveillance in public places (the issues of homes is often addressed in this context), with satellite video surveillance, with RFID, with data relating to living conditions in houses (such as water and electricity bills), and with heat

surveillance and other forms of scanning the home from the outside. Related to the latter, Article 13, paragraph 1 of the German Constitution (Grundgesetz) – 'The home is inviolable' – has been complemented with a paragraph to allow the use of wiretaps, bugs, and similar equipment in homes for fighting organised crime 'provided that alternative methods of investigating the matter would be disproportionately difficult or unproductive'. Similar issues in other countries have given rise to case-law. The Belgian Constitutional Court made it clear in 2004 that police competences to use bugs in houses needed to fulfil all the requirements of regular physical searches. In *Plant*, the Canadian Court accepted an inquiry of the police, who suspected drug cultivation, to the electric-utility company to have data on the use of electric power, because there was no trust relation between the owner and the company. The protection of the home in Section 8 Canadian Charter did not apply, because the electric reader did not reveal data on lifestyle but gave only primitive data. In *Kyllo*, the US Supreme Court saw a Fourth Amendment violation in the warrantless use of heat scans that monitored homes from the outside with devices not in general use. In *Teslin*, the Canadian court reached an opposite conclusion, arguing there was no reasonable expectation in heat that could be registered from outside homes; this technology did not reveal intimate details of lifestyle. This judgment seemingly contradicts the *Kyllo* findings, but the Canadian Court left the door open to find a reasonable expection of privacy in relation to more sophisticated technology. An issue not yet addressed in case-law is to what extent the inviolability of the home protects against hacking into or searching, by means of a network connection, personal computers located in the home.

Both observations give rise to two questions that should be answered by constitutional legislators. First, are the spatial dimensions of terms such as 'home', 'search', and 'illegal trespassing' technology-proof given the new means of monitoring the home from the outside in increasingly intrusive ways?[19] Second, what exactly is being protected by the inviolability of the home: the place or the people? Property, liberty, or privacy, or a combination of all these? It is important to take a stance on this, with a view to longer-term developments like domotics, which make homes 'intelligent' and therefore more revealing of intimate life to outside snoopers, and Ambient Intelligence, where a personalised environment follows individuals as they move around, rather than that individuals have a fixed geographical basis for a private sphere in the form of their physical home. In the long run, the notion of 'home' may need to be adapted itself to denote the personalised sphere around an individual rather than a fixed, brick-and-mortar place.

9.3.4. Inviolability of the body

The body is explicitly protected in the Constitutions of Canada, Germany, the Netherlands, and Sweden. The Belgian Constitution was amended in 2000 with a provision on the rights of children that includes protection of the body of the child. Other notions protecting the body are human dignity (France, Belgium), the right to life

[19] Cf., Koops, et al. 2004.

(Belgium), privacy (US, Belgium), and the privilege against self-incrimination (US)[20]. Canadian and German constitutional case-law suggest a high level of protection accorded to the body and to data related to the body. Canadian courts apply the rule that the closer something can be tied to the individual, the higher the expectation of privacy and the protection of the body. Thus, a handbag receives more protection than a school locker or a gym bag.

The right to have the body protected has not triggered many technology-related debates. Most debates, for example, about taking DNA samples, electronic monitoring of detainees, and using biometrics, have been conducted in the context of the general right to privacy and to ordinary data-protection legislation.

The notion of protection of the body is, however, particularly relevant for biomedical issues. Here, German and French law seem to be more principled and less pragmatic in their approach than the US, Sweden, and Belgium. The former systems let the notion of human dignity play a central role in these issues. In Germany, this right is rooted in the Constitution, whereas in France, it is recognised as a 'guarding principle' for constitutional rights and has been firmly incorporated in the Civil Code since 1994 (*Bioethics Act*). Although it is not easy to determine whether the more principled approach of some systems or the more pragmatic approach of other systems is to be preferred, it is beyond doubt that, when endeavouring to involve constitutional rights in a more active way in biomedical developments, recognising human dignity can complement the right to protection of the body. It should, however, be noted that human dignity can be interpreted in a more or in a less liberal way. The current German interpretation, for example, prevents liberal abortion laws and gives heightened constitutional protection to the embryo, in contrast to the current European human-rights framework.[21]

9.4. Communication-related rights

9.4.1. Secrecy of communications

The right to secrecy of communications is explicitly recognised at the constitutional level in Germany, Sweden, and the Netherlands. Whereas the Netherlands protects letters, the telephone, and the telegraph (Art. 13 Gw), the former countries use a sufficiently technology-neutral formulation: 'the privacy of correspondence, posts, *and telecommunications*' (Germany) and 'mail *or other confidential correspondence*, (…) telephone conversations *or other confidential communications*' (Sweden) (emphasis added). In Belgium and France, the secrecy of communications is not regulated at the constitutional level but by lower legislation; Belgium only provides a constitutional protection of mail (letters). In Canada and the US, the secrecy of communications has been read into the constitutional protection against unreasonable search and seizure. In

---

[20] This may also be the case in Europe, where the European Court of Human Rights found the administering by the police of an emetic (vomitive) to the applicant, who was suspected of having swallowed drugs, a violation not only of the right to be protected against inhuman or degrading treatment (Art. 3 ECHR) but also a violation of the privilege against self-incrimination (Art. 6 para. 1 ECHR). See ECtHR 11 July 2006 (*Jalloh* v. *Germany*).

[21] See also, in general, comparing a utilitarian, a human-rights, and a human-dignity approach to addressing biomedical-ethical issues and warning against a too principled 'dignitarian' approach, Somsen 2006.

Canada, e-mail falls within the scope of this protection, albeit to a lower degree than letters, but in the US, constitutional protection of e-mail is still undecided. This is similar to France, where the protection of e-mail in ordinary legislation, as interpreted by the Constitutional Council, depends on the circumstances. In these countries, encryption of e-mail is likely a sufficient condition to invoke legal protection, but it is not a necessary condition: depending on other circumstances, unencrypted e-mail can also be considered secret.[22]

As with the inviolability of the home, it is relevant to consider the exact nature of what is being protected: the communication itself, the place where the communication takes place, or the medium over which the communication is transported? The importance of this issue is borne out by the Dutch discussions, where different interpretations of the nature of the protection lead to differing proposals for reformulating the constitutional provision.[23] The US approach, similar to the Canadian approach, that the Fourth Amendment protects 'people, not places' was established in the *Katz* decision on wiretapping. This remark referred, however, primarily to the place where the interception occurred: a public phone booth, arguing that people can have a reasonable expection of privacy even in a public space. This gives little guidance as to the core of the protection, but it is presumably closer related to protecting the sender or recipient of a communication and the communication itself than to protecting the medium transporting the message.

The German approach differs in this respect. The German Constitution protects the confidentiality of individual communications that depend on a third party for transmission; it principally covers all forms of mediated communication for the period of the transport. It is, hence, the channel that is protected rather than the communication as such. The French protection in ordinary legislation seems to be based on the same approach of transport protection. This 'channel' approach has advantages in that it provides more legal certainty what kind of communications are protected, namely all communications transported across media that are protected as such, like the telephone. In the 'communication' approach, the medium is neither a sufficient nor a necessary condition: protection has to be determined on a case-by-case basis, by looking at all relevant aspects of the communication itself. A channel approach is, however, more difficult to maintain as media converge. This is visible in Germany, where only individual communications are protected and not mass communications (such as broadcasts): this distinction is blurred now that communications infrastructures converge (e.g., narrowcasting on TV infrastructures, broadcasting on the Internet, and types of communication on the Internet, such as blogging or communicating in large-scale but 'closed' communities like Hyves, that are not easy to call individual or mass).

On the basis of the chapters, it can therefore not be recommended to choose either a 'communication' approach or a 'channel' approach, but it is advisable that constitutional legislators at least make an explicit and argued choice in this matter, to provide as much legal certainty as possible in this complex area.

---

[22] Compare the *Weir* case in Canada, *supra* 3.5.1.

[23] See *supra* 6.5.1.

Traffic data and data retention

A relevant issue is to what extent the constitutional protection of secrecy of communications covers traffic data (such as number, time, and – with mobile communications – location of a call). Generally, the reporting countries make a distinction between the content of communication and traffic data. There seems to be a traditional tendency in most countries to consider the latter less privacy-sensitive than the former, although the literature in some countries increasingly argues that traffic data should be considered equally privacy-sensitive.[24] In Germany and Belgium, traffic data fall within the scope of secrecy of communications (Art. 10 GG, Art. 122 et seq. Belgian Electronic Communications Act of 2005).[25] In the Netherlands, however, traffic data are seen as part of privacy and data protection instead (Art. 10 Gw). In Canada and the US, traffic data are treated – like the content of communications – in the context of unreasonable search and seizure, but with different outcomes: whereas the US denies constitutional, Fourth Amendment, protection to traffic data outright, Canada assigns some constitutional, Section 8, protection to traffic data, albeit to a lower extent than communication content.

Given these varying constitutional approaches, it is hard to recommend how exactly traffic data should be protected at the constitutional level; perhaps it is ultimately a matter of choice to be made in light of the national interpretation of rights to secrecy of communications, privacy, data protection, and protection from unreasonable search and seizure. It should also be noted that, however varying the constitutional approaches may be, the material protection for traffic data does not necessarily differ that much in practice, since it is usually provided by ordinary legislation; the US ECPA, for example, offers more protection than the Fourth Amendment *Katz* standard.

A topical issue is data retention: the requirement for telecommunications providers to store traffic data for a certain period, as a measure to combat serious crime and terrorism. Significantly enough, this measure is only taken in Europe, with the 2006 Data Retention Directive;[26] it does not feature in the US anti-terrorism PATRIOT Act, and there are no proposals considering data retention in the US or in Canada. In Europe, France and Belgium had enacted data-retention legislation before the EC Directive. In France, the application Decree bringing into force this part of the Daily Safety Act was published in 2006, and ultimately approved by the CNIL as being constitutionally acceptable, given the limitations in the law of purpose-specification and duration. In Belgium, the implementing decree for Article 126 Electronic Communication Act is still in preparation. Germany, the Netherlands, and Sweden will have to draft implementation laws. From a constitutional perspective, it is relevant to note that a motion was rejected by the German Parliament to request the government to challenge the directive at the

---

24 In the context of the Lawful Access Initiative in Canada, scholars argue that traffic data can be just as privacy-sensitive as the content of communications, see *supra* 3.5.1. In the Dutch context, see *supra* 6.5.1; also cf., the annotation by Egbert Dommering under ECtHR 25 September 2001 (*P.G. & J.H.* v. *United Kingdom*), *Nederlandse Jurisprudentie* 2003, No. 670, available at http://www.ivir.nl/publicaties/dommering/ehrm25sep2001.html.

25 Cf., the European Court of Human Rights, which treats traffic data as part of the right to respect for 'correspondence' in Art. 8 ECHR. See, e.g., ECtHR 2 August 1984 (*Malone* v. *United Kingdom*) and ECtHR 25 September 2001 (*P.G. & J.H.* v. *United Kingdom*).

26 European Directive 2006/24/EC of 15 March 2006 on data retention.

European Court of Justice,[27] but that several groups and individuals have announced to challenge the future German transposition law before the Constitutional Court.[28]

9.4.2. Freedom of expression

The freedom of expression is an important constitutional rights in all reporting countries. The scope of the right differs, however. In France, the Netherlands, Sweden, and the US, the right focuses on the *expression* or *communication* of thoughts and opinions. Canada has a more encompassing right, covering also the freedom to *hold* thoughts and beliefs; Belgium is similar in that it creates the freedom of expression along with the freedom of worship (Art. 19 Belgian Constitution). Germany also stipulates a constitutional right to *gather* information, to stimulate the forming of thoughts and opinions.

Despite the overall importance of the freedom of expression and the largely similar culture in the reporting countries to favour openness and public debate over censorship, each country distinguishes certain types of speech that are excluded from protection. Several of these are shared by most countries, such as – in the US terminology – 'true threats', defamation, and child pornography (in all reporting countries), and hate speech (in all except the US). Other categories are more specific for certain countries, such as political speech (banned in Canada in the 20-hour period preceding the closing of polls, given the vastness and time zones of the country), court proceedings (which in certain cases cannot be published in Canada), and commercial speech (which has a lower standard of protection in the US and is completely excluded in the Netherlands). For virtual child pornography, it is noteworthy that a US law banning this was struck down as unconstitutional; the constitutionality of a subsequent, more strictly formulated but functionally equivalent, criminalisation has so far not been decided in court. In the other reporting countries, several of which have also criminalised virtual child porn in the wake of the Council of Europe's Convention on Cybercrime, the constitutionality of these prohibitions does not seem to be an issue.

Particularly relevant in the context of this report is the freedom of media that express or transmit opinions. Article 7 para 1 of the Dutch Constitution specifically addresses freedom of the press, whereas para 2 deals with broadcasting through radio and television and para 3 protects other means of expression. It is unclear if, and if so under which provision, expression of ideas and opinions by means of digital media such as the internet, is protected. In case-law, the courts include both Article 7 Gw and Article 10 EHCR into their consideration without specifying which part of Article 7 applies. Article 25 of the Belgian Constitution is restricted to freedom of the press, which tends to be associated with the printing press, and courts are reluctant to interpret this to cover new media. The US First Amendment also only mentions freedom of the press, but this is interpreted much more broadly than in Belgium, and there is no debate that the right is formulated in too technology-specific a way. The German Constitution, in Article 5,

---

27 See http://dip.bundestag.de/btd/16/016/1601622.pdf.

28 See http://www.edri.org/edrigram/number4.10/dataretentionde. Outside the scope of this survey, but relevant to note in this respect, is the case brought before the Irish High Court against the Irish government by Digital Rights Ireland, challenging the Irish data-retention law and the EC Directive as unconstitutional. See http://www.digitalrights.ie/category/data-retention/.

mentions the freedom of the press and the freedom of reporting by means of broadcasts and films, thus distinguishing the press from audiovisual media. Given a similar distinction in French ordinary legislation, the Internet has triggered a restructuring of French media law, which now has a general category of 'electronic public communications', which is divided in two sub-categories: 'audiovisual communications' (subject to the Freedom of Communications Act), and 'on-line public communications' (subject to the Trust in the Digital Economy Act). Canada and Sweden have no problems with new technologies, since they use open-ended formulations: 'and other forms of communication' (Canada), 'and certain like transmissions, (…) and other technical recordings' (Sweden). Nevertheless, given the fact that Swedish constitutional protection of freedom of speech is spread across two constitutional laws, the Freedom of the Press Act and the Fundamental Law on Freedom of Expression, an inquiry is on-going to merge these laws.

The Internet raises several questions with respect to the freedom of expression. A primary topic is the categorisation of bloggers. On the one hand, they serve a purpose very similar to journalists in the printed press, by fostering the collection and spreading of information, ideas, and opinions, and therefore may well, in the longer term, turn out to be equally valuable for the public debate as traditional media, or perhaps even more valuable. On the other hand, on the Internet, everyone can start a blog and call herself a journalist. The reporting countries are tentatively coming to terms with defining bloggers. In Belgium, the criterion of 'everyone who directly contributes (…) information aimed at the public via a medium' has been formulated to trigger applicability of the Act on the protection of journalistic sources, thus in principle covering bloggers as well. In Canada, courts tend to apply a broad definition of journalism as well in relation to new media.[29] In Sweden, a more material criterion is used, namely that information be 'of importance to the public debate' in order to be protected by the freedom of expression;[30] this allows courts to assess bloggers – and other expressers of opinions on new media – on a case-by-base basis in light of the rationale of the constitutional protection. With converging media, this seems a more sustainable approach than a media-centered type of protection.

Other interesting Internet-related issues with respect to the freedom of expression are the distinction between static and interactive websites (in Sweden, only static websites fall within the scope of the Fundamental Law on Freedom of Expression), the liability for hyperlinks that link to prohibited speech (Germany: no liability because the hyperlinker aimed at faciliting people to form an opinion; France: liability because the hyperlinker had explicit knowledge of or advertised the linked content), the liabiliity of ISPs (in France, the Netherlands, and Canada), the impact of search engines (the Netherlands), and filtering systems (Canada). Also noteworthy are the activities in France and Belgium for the protection of minors on the Internet.

On the basis of the reports, it can be recommended that the freedom of expression – possibly strengthened by the freedom to gather information and to hold beliefs and opinions – is formulated in a sufficiently media-neutral way. An enumeration

---

[29] Jason Young, communication at the 1 December 2006 workshop.

[30] Cecilia Magnusson Sjöberg, communication at the 1 December 2006 workshop.

of media with an open-ended formulation – like the Canadian 'and other forms of communication' – seems particularly apt to strike a balance between legal certainty (for media that should be protected in any case) and technology neutrality (for media that may also need to be protected, perhaps through future technological developments). Given the increasing convergence of media and the rise of new ways of expression, such as blogging, that blur traditional concepts like 'journalist', it is also useful to consider including, besides or instead of the mentioning of media, a material criterion, such as 'of importance to the public debate', that judges can use to decide whether in a concrete case a communication serves the values underlying the freedom of expression.

9.5. Other and new constitutional rights

The chapters have also mentioned several other constitutional rights as being affected by new technologies. Apart from the right to anonymity, which all reporters touched upon as it closely relates to both privacy and freedom of expression, and which we therefore treat separately in this section, no general conclusions can be drawn from the chapters, since the reporters were asked to focus on the privacy-related and communications-related rights and to go into other rights only as far as time and expertise were available.

9.5.1. Right to anonymity

Although anonymity is a topic of debate in all reporting countries, none of the countries acknowledges a general right, constitutional or otherwise, to anonymity. It is, however, often a subsidiary or a derivative of constitutional rights. There exists, to some extent, a constitution-related right to anonymity in the context of privacy (in France), data protection (in the form of the right to informational self-determination, in Germany), the secrecy of communications (in Germany), free speech (in the Netherlands, Canada, and the US), and the right to individual liberty (which, in France, includes the freedom to come and go anonymously). This right is far from absolute: numerous exceptions are made, such as a legal obligation for bloggers to inform the hosting provider of their identity (France), a ban on equipment that obstructs caller-identification in telecommunications (Belgium), and a prohibition of anonymous political advertising (Canada). Also, discussions about revealing the identity of unknown or pseudonymous Internet users alledgedly infringing copyright or committing a content-related crime online, can be witnessed in all countries, often allowing the lifting of anonymity of the purported offender. A conclusion that can be tentatively drawn from this overview is that anonymity tends to be protected in most countries as a not unimportant value, also at the constitutional level, but that infringements of anonymity are generally easily accepted. It is therefore not possible, on the basis of the chapters, to conclude that a 'right' to anonymity exists; rather, it plays a role as a value in the context of several other constitutional rights.

9.5.2. Various

Various constitutional rights and issues are mentioned in the chapters as being potentially affected by new technologies. We give a brief overview here.

The freedom of assembly is possibly relevant for on-line demonstrations or virtual sit-ins, as was argued by the Dutch CFRDA; however, a lower court in Germany declined applicability. The freedom of association can apply to new media, although banning associations from a virtual game by game providers might be quite lawful (as argued in Dutch literature). The right to petition 'in writing' was interpreted in the Netherlands as also covering petitions by electronic means. Equal treatment (Art. 10-11 Belgian Constitution) was an issue in Belgium when the Official Journal (*Belgisch Staatsblad*) was transformed into an on-line publication, impacting the accessibility of the journal in an unconstitutional way. Computer games raise questions about the applicability of personality rights, such as portrait rights, and the freedom of art; a German lower court held that a computer game could claim the constitutional right to freedom of art, but the appeal court found that even so, a celebrity's consent was needed to use his name in the game. In the United States, a right to experimental, potentially life-saving, medication was invoked even if the drugs had not passed all tests for FDA approval. In France, the right to be forgotten is mentioned for underage offenders.

In the criminal-law context, the criminal legality principle (no crime without prior law, Art. 12 Belgian Constitution) is relevant in that it requires precise law-making, so that citizens can foresee what is punishable and how they can be investigated. In the Belgian Computer Crime Act, the formulation of 'any other technological means' was used in an attempt to make the description technology-neutral. This meets the legality principle on the face of it, since all 'technical' crimes are covered, but at the same time, foreseeability is not guaranteed with such an open ending. Also in the criminal context, in the US, the privilege against self-incrimination (Fifth Amendment) is relevant in relation to technology, for instance in the context of a power to compel citizens to hand over encryption keys. Brenner argues that such a power would violate the Fifth Amendment unless the key (or password) was reduced to tangible, recorded form. Saliently enough, such a power, which has not been enacted in the US, does exist in France and Belgium, but in these countries, the power to force suspects to decrypt has so far not been challenged as infringing the privilege against self-incrimination.[31]

In the context of electronic government, various issues spring to attention. Notable first of all is the right to access public information, which is a constitutional right in both Belgium and Sweden; in the Netherlands, a Bill to introduce this right in the Constitution is expected. Whereas the Dutch proposals speak of 'public information', the other countries use the term 'document'. In Belgium, this has been interpreted broadly to cover all kinds of documents regardless of the storage medium, whereas in Sweden, the term 'recording', used alongside 'written or pictorial matter' in the definition of 'document', refers to electronic documents. 'Recordings' in Sweden can be ready-made (such as e-mail messages) or compilations (like merged data bases); compilations only fall within the scope of the right to access public information if the government can make them accessible 'using routine means'. In Sweden, also the storage and deletion of official electronic documents has been called attention to in the context of the right to access public information.

---

[31] The privilege against self-incrimination is not always recognised at the constitutional level in European countries, but it is at the core of the constitutional right to a fair trial as interpreted by the European Court of Human Rights, since its first acknowledgement in ECtHR 25 February 1993 (*Funke* v. *France*).

Another relevant rights in the context of e-government is the right to vote. In Belgium, the law was adapted in 1998 to allow voting machines, without debate; in the US, a few civil-law suits arguing that flawed voting machines violated their right to vote were denied. E-voting has been discussed and briefly experimented with in France as an alternative to distance-voting. In the Netherlands, which has a long history of using voting machines, serious debates about secrecy of the ballot have only started in 2006 as a result of studies regarding the security measures of these voting machines and the possibilities of secretly eavesdropping on the votes cast.

Finally, a fundamental issue outside the field of human rights has been raised in the Swedish chapter. The power to enact laws is constitutionally attributed to the legislator (the Riksdag, and sometimes the Government or by delegation another public authority). The increasing use of computer-assisted and computer-executed legal decisions, notably in the field of administrative law, raises the question whether and to what extent the programs used for these decisions, in which rules are embedded, should be seen as enacted laws. After all, the legal rules of law proper are not trivially translatable into technical, computer-logical rules, and hence, programming constitutes a degree of autonomous rule-making. This requires a check on the conformity of the resulting program rules with the legal rules and on the constitutional authority underlying the technical rule-making process. Related to this is the issue in Sweden of the distribution of competence between local and central authorities: if administrative decisions are largely the result of centralised information systems, the constitutional task of local governments to take indivdidual administrative decisions is at risk.

9.5.3. Conclusion

Although no general conclusions can be drawn from this brief overview, two observations can be made on the basis of the mentioning in the chapters of other rights. First, the challenges that new technologies pose to constitutional law are wide-ranging and go deeper than merely the occurrence of technology-specific formulations in constitutional provisions. The issues mentioned range from traditional, age-old constitutional rights like the freedom of assembly and the right to vote to more recent or even new rights, such as the right to access government information and the right to be forgotten. What is more, they also relate to constitutional issues outside the field of human rights, such as the division of power within the government.

Second, despite the wide range of issues touched upon, the issues signaled by and large relate to developments in the near rather than the distant future, and they tend to involve ICT rather than other new technologies. This may well be caused by the background of the reporters, all of whom have a track record in the field of ICT law in particular, but it could also be an indication that biotechnology and genetics, nanotechnology, and the convergence of nano, bio, information, and cognitive sciences (NBIC) have as yet caused little discussions in relation to constitutional rights. The long-term impact of these developments on fundamental issues, for example, whether cyborgs and robotics necessitate a rethinking of the concept of the bearer of constitutional (‘human’) rights, or the effect of NBIC on legal notions based on the concept of free will, has to our knowledge not been discussed in any detail in literature or in constitutional-policy debates.

9.6. Conclusion

New technologies challenge constitutional rights. This is particularly visible in the Dutch context, where the technology-specific formulation of several constitutional rights necessitates an adaptation of the Constitution. In the other countries covered in this report, however, the text of the Constitution itself is hardly at issue. In some countries, a few adaptations have been made to bring the formulation up-to-date in light of new technologies, but no such adaptation has occurred since 2000, and no need is currently felt to adapt the Constitution – with the possible exception of the Belgian freedom of the 'press'. Generally, constitutional rights are sufficiently technology-neutral, because they are abstractly worded or use open endings (notably in Sweden), use guiding principles like a general right to personality (Germany), or are kept up-to-date by constitutional or other courts who can interpret the rights by deviating from a literal reading (US, Canada). Constitutional review is also, in varying forms, a primary feature of all except the Dutch constitutional systems covered in this report that explains the lack of need to modify the constitution itself.

Besides a lack of constitutional amendments, a general trend is perceptible of low constitutional dynamics. Some countries, notably Belgium, have seen a relatively vibrant constitutional activity in the past few years, with a full-blown Constitutional Court as a result, but in most countries, constitutional rights do not seem to play a key role in debates over new technologies, at least, on the face of it. [32] A second look at many of the issues covered in this report shows that constitutional values related to privacy and freedom of communication do feed technology-related policy, legislation, and case-law, but often without reference to specific constitutional rights. In other words, constitutional values are important for technology policy and law, but in an indirect way: they often play a role in an implicit way, and through other, non-constitutional legislation that embeds and implements constitutional rights.

This is hopeful, because new technologies pose challenges, if not to Constitutions as such, to all areas of the law. In shaping the law and legal policy to face future, technology-related developments, constitutional values are urgently needed to help guide society through a process that will certainly bring radical changes, particularly since it is hard to foresee which changes exactly will be brought about by new technologies. Constitutional rights are core values that define what human beings and society are and should be. Therefore, even if constitutional rights are far from dormant, legislatures and policy-makers would do well to more explicitly refer to constitutional rights in their activities, and to create an environment in which constitutional rights can flourish and guide society along.

References

ASSCHER 2002

[32] About the differences in style and rhetoric between American and European constitutional courts: Lasser 2004; Rosenfeld 2006. Both authors show that compared to the American Court, European courts within the French tradition tend to speak in one, abstract voice. The Supreme Court is more prone to focusing on a multitude of 'factors' and 'considerations' when tackling constitutional issues. Due to these differences of style, it is therefore more difficult to learn about the actual difficulties presented by constitutional issues at stake when reading European constitutional judgments.

L. Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving* [Communications-Related Constitutional Rights] (Amsterdam, Otto Cramwinckel 2002).

BLOK 2002

P. Blok, *Het recht op privacy* [The Right to Privacy] (Den Haag, Boom Juridische uitgevers 2002).

DE HERT 2004

P. De Hert, 'Division of Competencies Between National and European Levels with Regard to Justice & Home Affairs', in J. Apap, ed., *Justice and Home Affairs in the EU. Liberty and Security Issues after Enlargement* (Cheltenham (UK), Edward Elgar Publishing 2004) pp. 55-102.

LASSER 2004

M. de S.-O.L'E. Lasser, *Judicial Deliberations, A Comparative Analysis of Judicial Transparancy and Legitimacy* (Oxford University Press 2004).

FRANKEN AND KOEKKOEK 2006

H. Franken and A.K. Koekkoek, 'The Protection of Fundamental Rights in a Digital Age', in International Academy of Comparative Law (Brussels, Bruylant 2006) pp. 1147-1164.

KOEKKOEK, ET AL. 2000

A. Koekkoek, et al., *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport* [Protection of fundamental rights in the digital age. A comparative study of the freedom of information and of communication and privacy in Sweden, Germany, France, Belgium, The United States of America and Canada] (Tilburg, Katholieke Universiteit Brabant 2000).

KOOPS 2006

B.J. Koops, 'Should ICT Regulation Be Technology-Neutral?', in Koops, et al., eds., *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners* (The Hague, T.M.C. Asser Press 2006) pp. 77-108, available at http://papers.ssrn.com/abstract=918746.

KOOPS 2002

B.J. Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy* [Criminal Investigation of (Tele)communications 1838-2002] (Deventer, Kluwer 2002).

KOOPS AND LEENES 2005

B.J. Koops and R. Leenes, '"Code" and the Slow Erosion of Privacy', *Michigan Telecommunications & Technology Law Review 12* (2005) pp. 115-188, http://www.mttlr.org/voltwelve/koops&leenes.pdf.

KOOPS, ET AL. 2004

B.J. Koops, et al., *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken* [Seeing Right Through. Exploring the Future of Inviolability of the Home and the Body and New Investigation Techniques] (Den Haag, Sdu 2004).

NOUWT, ET AL. 2005
Sjaak Nouwt, et al. (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (The Hague, T.M.C. Asser Press 2005).
ROSENFELD 2006
M. Rosenfeld, 'Comparing constitutional review by the European Court of Justice and the U.S. Supreme Court', 4 *International Journal of Constitutional Law* (2006) pp. 618–651.
SOMSEN 2006
H. Somsen, *Regulering van humane genetica in het neo-eugenetische tijdperk* [Regulating Human Genetics in the Neo-Eugenic Era], inaugural lecture Tilburg (Nijmegen, Wolf Legal Publishers 2006).